DOCUMENT RESUME

ED 232 174 CS 207 671

AUTHOR Dalsey, John F.
TITLE The Relationship between Law, Privacy, and Information Technology: A Legal and Philosophical Inquiry.
PUB DATE 83
NOTE 31p.; Paper presented at the Annual Meeting of the Association for Education in Journalism and Mass Communication (66th, Corvallis, OR, August 6-9, 1983).
PUB TYPE Speeches/Conference Papers (150) -- Viewpoints (120)

EDRS PRICE MF01/PC02 Plus Postage.
DESCRIPTORS *Civil Liberties; Computers; *Court Litigation; Information Storage; *Information Systems; Legal Problems; *Legislation; Media Research; *Privacy; *Technological Advancement
IDENTIFIERS *Computer Managed Information; Computer Networks; Information Industry

ABSTRACT

Historically, legislation or judicial review successfully controlled threats to personal privacy by information technology. Wiretapping legislation, for example, developed along with sophisticated telephone equipment. Today, however, the law is unable to respond quickly enough to the constantly changing situations and behaviors created by massive computerization. Based on a paper concept of information, even such recent legislation as the Privacy Act of 1974 cannot address problems arising from the permanence and universality of computerized personal records. Not only legislation, but traditional common law, applicable in only certain situations and requiring proof of personal injury, is no longer viable in many contexts. If technology's impact on the individual is to be controlled, laws must be developed to cope with the future, instead of to simply reflect the past. The concept of personal autonomy must be refined to include control over the image presented. To that end, society should avoid loading computers with personal data, monitor the transmission of personal records between computer systems, and create lawyers able to adapt to the changing legal issues and categories brought about by technological advances, who will defend the individual's right to privacy. (MM)

****
* Reproductions supplied by EDRS are the best that can be made *
* from the original document. *
****

ED232174

THE RELATIONSHIP BETWEEN LAW, PRIVACY, AND INFORMATION TECHNOLOGY: A Legal and Philosophical Inquiry

by

John F. Dalsey, J.D.

Franklin Pierce Law Center

"PERMISSION TO REPRODUCE THIS MATERIAL HAS BEEN GRANTED BY

John F. Dalsey

TO THE EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)."

U.S. DEPARTMENT OF EDUCATION
NATIONAL INSTITUTE OF EDUCATION
EDUCATIONAL RESOURCES INFORMATION CENTER (ERIC)

X This document has been reproduced as received from the person or organization originating it.

☐ Minor changes have been made to improve reproduction quality.

• Points of view or opinions stated in this document do not necessarily represent official NIE position or policy.

Copyright © 1983 by John F. Dalsey

CS 207 671

THE RELATIONSHIP BETWEEN LAW, PRIVACY, AND INFORMATION TECHNOLOGY: A Legal and Philosophical Inquiry

By John F. Dalsey

INTRODUCTION

Technological innovation is inextricably linked to the evolution and survival of the human race. It fashions what it is that we become. For example, when man first began to use simple tools, he was forced to rely on a bipedal form of locomotion. The better he learned to walk: the more he used his hands. The more he used his hands: the better his toolmaking ability became. The use of tools encouraged the application of abstract reasoning to the task of hunting and gathering and led to the development of a larger brain. Our self awareness and our forms of social organization were made possible by the technological process. That process is the purposeful marrige of mind and matter: through it, we manipulate the world around us in order to achieve ends. To this day, technology continues to play a significant part in the nature of our evolution./1/

In retrospect, we see how the scraper, axe, and spear promoted the

organizational abilities and effectivness of hunting and gathering societies. We see how man's ability to store information in his mind about the natural world, process it, recall it, and communicate to others gave rise to more complex social organizations. But not until mankind applied the technological process to communication, did civilization appear. Particularly, it was through early forms of written communication that the organization and control of civilized society became possible. The technology of the written word had a tremendous impact on human relations. Law as we know it remains a product of that revolution in information technology: the written word.

Although we can see the impact of the written word upon the development of civilization, could the earliest scribes? Could they have possibily imagined? The aim of this article is to ask the same question of ourselves about the current revolution in information technology and the increased incorporation of the computer and its related technologies into our lives. Just as the scribes were on the threshold of a new age as a result of their information technology, so are we.

The emergence of, and reliance upon the computer and its related technologies is having a pervasive economic, social and political effect upon society. Rapid advances in information technology present novel legal and social policy questions involving important human values. The way in which we choose to adapt or to control information technology through the law will have a significant impact on our future rights and liberties as individuals in society. Yet the traditional evolutionary processes of the law, both in defining and in resolving new problems,

remain suited to a simpler age. It is important that we now come to a deeper understanding of the law and of our political ideals, and that we examine the relationship between law and technology in order to define emerging problems and propose meaningful solutions. This is particularly true in the area of privacy, which is a poorly understood and confusing topic in law.

What is privacy? What are rights to privacy? How should the law control the revolution in information technology? Should the law control the technology or its use at all? To address these questions is to make a serious inquiry into the law, what it is that we are, and what it is that we want (or don't want) to become.

THE RELATIONSHIP

This paper will examine the relationship which exists between law, privacy and technology. Law is the institution with which we respond to or control technology, especially when the technology poses an uncertainty involving human values. Law has been responding to information technology for a long time. In most every instance, the response has been related in some way to the concept of privacy. But "privacy" remains the legal name for a poorly understood bundle of values. Definitions of privacy abound. They can be found in statutes, case law, philosophical treatises, psychological journals and legal literature. Consider the following definitions.

Privacy is:

the right to be let alone.

the right of personality.

a person's feeling that others should be excluded from something which is of concern to her or him, and also recognition that others have a right to do the same.

a value to be oneself; relief from the pressure of the presence of others.

the individual's seclusion from public affairs.

an outcome of a person's wish to withold from others certain knowledge as to his or her past and present experience and action and his or her intention for the future; a desire to be an enigma to others or to control other's perceptions and beliefs about oneself.

a psycho-sociological right, not a legally recognizable right.

freedom from intrusion into one's solitude, seclusion, or personal affairs.

freedom from the public disclosure of embarrassing private facts.

freedom from the use of a person's name or likeness in a false light.

freedom from the appropriation of a persons name or likeness for an unauthorized commercial use.

the control over access to information about oneself.

an existential condition that can be described; it is not a right or claim.

created by expectation.

a liberty and a natural right.

a right to be free from unwarranted governmental intrusion.

an interest: (1) in avoiding disclosure of personal matters; and (2) in making certain kinds of important decisions. /2/

Emergence of the "Law of Privacy".

It is frequently stated that privacy is a relatively new legal concept. However, this is not the case. Both ancient Jewish and Roman law recognized that the violation of another's privacy was a legal and moral wrong. Jewish law declared explicitly that the harm of being seen in private is a legal wrong. In Roman law, "injuria" meant any willful disregard of the personality of another or injury to honor, the insult being the essential point, not the injury to the body./3/

Similarly, the codified and monarchial law of Europe recognized that any unauthorized invasion into the privacy of another is an actionable wrong. German and Swiss law refer to the "sphere" of individual privacy./4/

American common law recognized a right to privacy at about the turn of this century. One of the earliest privacy cases was Pavesich v. New England Life Insurance Co./5/ This case arose out of the unauthorized use of a person's picture by an insurance company for advertising purposes. The court decided to award damages to the person whose picture was used on the basis of a right to privacy theory. It was described as the right to be let alone and to be protected from unauthorized publicity in one's essentially private affairs. The reasoning in the opinion was based on an article about privacy written by Warren and Brandeis in 1890./6/ The reason this case became the subject of a law suit reveals something about the relationship between law, privacy and information technology.

Is Technology the Driving Force Behind the Right to Privacy in the Common Law?

Prior to the early twentieth century, society was such that adequate protection of a person's privacy with respect to information was afforded through property rights, defamation and contract law. It was not until technological advances made photographs and inexpensive printing and paper available that a 'right to privacy' was judicially recognized in the United States. Technology created a new type of problem involving human values and relationships and the law responded. The early developments in information technology created a situation in which law responded by creating and defining a set of rights to control it.

We see that law responded to the Pavesich situation by creating a set of rights. This response was appropriate in its age. Prior to the early 1900's the pace of technological development was not too rapid for this quite ordinary evolutionary process of the law to work. After Pavesch, however, it took over thirty years for a majority of states to recognize a right to privacy through the common law. To this day, two or three states have not yet recognized the right to privacy./7/ Also, it should be noted that the creation of a rights based approach adequately dealt with the problem presented by the technology at the time. Individuals could

easily determine when they had been harmed under the law and could bring a law suit in order to recover damages for invasions of privacy. The threat of law suits, for a while at least, deterred abuses of privacy and the application of technology towards wrongful ends as defined by society.

Problems with the concept of Privacy in Present American Society

Imagine the issues which confront society in connection with the latest developments in information technology. One author estimates that nearly half of the United States gross national product and half of the nation's wages are related to information technology industries./8/ Society is entering a new epoch, the age of information./9/ Information has a new meaning because of technology, both in the way it is gathered and in the way it is stored. Simply by participating in the mainstream of society, people leave an indelible trail of information about themselves Computerized information is permanent, universal in terms of transmitability and translatability, cheap to collect, and it is remote from us. We now live in a world where our actions are not transitory, and where our actions can be the subject of surveillance without our knowledge or consent.

Our world is full of concepts and technologies unimaginable just a few years ago. A good example of this is Landsat 4, the United States' newest

and most versitle earth-observing satellite. It circles the globe every 96 minutes from pole to pole taking electronic photos of every spot on earth with the exception of a small region around the poles. The Pentagon's spy satellite, Big Bird, can read the headlines of a newspaper from outerspace and instantly transmit the information back to earth./10/ Another example is "Net 2000": American Bell's newest computer translating and switching device. Through it, a computer can communicate with any other, regardless of the language the other computer speaks. Computers communicate over the telephone system as a routine matter in business every day.

The business of "selling" information in the private sector is a blossoming industry. Information is routinely collected and stored in data bases by private enterprises from all conceivable sources including public records kept by state and federal governments, news publications, wire services, banks, hospitals, insurance companies and credit bureaus. Such enterprizes sell the information to subscribers of their services, to private persons willing to pay for it, and in some cases, to the government./11/ Even information gathered from private citizen's garbage is analyzed, and stored in data bases by sociologists in several major universities. The University of Arizona has one of the nation's most extensive "garbology" programs.

Employers who use computers can now assess their employee's performance to a degree never before imaginable: a computer can be asked, for example, how many incorrect keys are struck by an operator in a given period of time, or how many bits of information were processed. Certainly, this

kind of surveillence lends itself to creating artificial differences in value or worth between workers and to creating psychological stress.

In Albquerque, New Mexico, a technological altervative to incarceration is being explored by the court system. Rather than serve time in jail, qualifying defendants found guilty of driving while intoxicated may report to the police station at the end of each work day and have a transmitter secured to their arm or leg. They must then go home and dial their phone to a special number; if they stray any farther than a few hundred feet from the phone, the transmission gets interrupted and the police are notified. In the morning, the person returns to the police station, has the transmitter removed, and goes to work again.

In the very near future, it is likely that computers will become as commonplace in the home and office as the telephone. The magnitude and diversity of information soon to be available through the home computer is staggering. Relations between people will occur within a new context and will take on new meaning.

The context and meaning of our relationships determines the course of our future and what it is that we become. Technology is rapidly changing the way in which people relate to each other and the way in which social controls can be implemented. Law must address this phenomena and guide and control it. The way in which this must be done is much more complex than the traditional rights based approach found in the common law.

The Common Law Rights-Based Approach to Privacy is a Product of a Simpler Age and is Now Impractical

A common law rights-based approach to the protection of privacy is no longer viable in many contexts. It requires that a person have standing, or be injured, in order to do anything about the right. Remedies for rights violations tend to be compensatory and limited to the facts of a particular situation. Technology is outstripping the current common law of privacy. This is due to the law's tendency to rely on prevailing custom for guiding principles . Common law is constrained further by the limitations of stare decisis /12/ and rigid categorical legal thinking. For example, the American common law formulation of a right to privacy is cast in terms of categories: commercial appropriation of a person's name or likeness, public disclosure of embarassing private facts, intrusions into a person's seclusion of soltitude, and using a person's name or likeness in a false light. However, changes in information technology have occurred rapidly, and are so sweeping in terms of impact on culture and societial values, that traditional common law cannot respond fast enough.

While the common law struggled with the right to privacy, the political process provided the legal response to the evolving technologies during most of this century. The invention of the telegraph gave rise to the Radio Communications Act of 1912 and the Radio Act of 1927. These Federal Statutes made it a crime to divulge or receive the contents of a radio

communiation without authorization. We see the emergence of copyright law and expanded notions of intellectual property by statute in response to advances in printing and reproduction technology. With the television: the FCC. With modern telephone communications: several forms of wiretap law. Finally, growing concern over the federal government's immense stockpile of personal information about individuals brought about the Freedom of Information Act (FOIA), the Privacy Act of 1974 and the Privacy Protection Act of 1980./13/ Likewise, many states have enacted laws that regulate the use and dissemination of information held by state governments./14/

We see in all of this, a traditional human concern with something that can be labeled privacy. The legislative process has acted in a forum where the judicial process could not act fast enough. Until recently, the legislative process has worked well. In most cases, the political-legal response to information technology was made in situations where the potential harms brought about by the technology were objectifiable and apparant. But the problems we face with emerging information technologies are not easily quantifiable and they give rise to serious questions about our rights as individuals. Technology is, for the first time, forcing us to re-examine our values and the underpinnings of our institutions./15/ Technology has outstripped the law.

Relations between people, business and government are taking on new forms. Computerized records, rather than the individual in person, form the basis in most cases for determining the way in which people are treated by businesses and governments. The laws which regulate the use of

information about people remain suited to a simpler age. Even the most recent statutory laws, the FOIA and the Privacy Act of 1974, are based on a paper concept of information. The Privacy Protection Commission concluded in a two year study:

> Current law is neither strong enough nor specific enough to solve the problems that now exist. In some cases, changes in record-keeping practice have already made even recent legal protections obsolete. As record-keeping systems come to be used to preclude action by the individual, a recent trend in the credit and financial areas, it is important that the individual also be given preventitive protection to supplement the after-the-fact protections he sometimes has today. . . .The law as it now stands simply ignores the strong interest many people have about records about them./16/

The FOIA and the Privacy Act make information available to the American public about the existence of most personal record keeping by the government. They also give individuals the means to assure the accuracy of such information, however, the laws seldom give an individual the right to challange the keeping of the information itself. These laws implicitly recognize that people should have some kind of control over information about themselves. This underlying theme was viable up to just a few years ago when computer technology was not such a common component of our culture. It was also viable when people had a meaningful choice about what information they released about themselves. However, the world is now a different kind of a place. Anyone who participates in the mainstream of society leaves an indelible trail of personal information about themselves. We know more about each other, but this knowledge is highly artificial. The government knows more about us. Communications satellites whirl above us beaming millions of bits of information about. The ears of world governments collect it all.

A new power is in the world. To have information is to have power. Having enough information about any given subject gives the holder of that information a strong potential power to control the subject. This concept is not a new one. History shows us that even the mightiest army's plans can be thwarted by effective surviellance by the enemy. There is now no limit to the amount of information that can be collected and stored in one place.

One of the major concerns of the founders of the United States was the balance of power between the major branches of government, and between the states and the federal government.

So far, in the area of power by information, the federal congress has demonstrated a marked tendency to resist the centralization of information in the federal government. For example, a 1965 study commissioned by the U.S. Bureau of the Budget proposed a Federal Data Center to centralize personal data collection. The House and Senate, responding to public uproar, wholeheartedly rejected the proposal. It was feared that such centralization of information would "depersonalize the American form of life"./17/ Subsequent attempts at the complete centralization of all information held by the federal government have also failed. However, considerable centralization does exist. For example, the Department of Health, Education, and Welfare is authorized to access many federal record systems to track down a parent who is not supporting his or her children. The FBI National Crime Information Center and the Social Security Administration Data Acquisition and Response System, are both nationwide computer systems which make information available to other governmental, and sometimes private, agencies./18/

The most notable exception in this discussion of power is the executive branch monopoly on communications surveillance. This area presents the most striking privacy issues, yet it is one in which there is little legal, and no social, constraint. The largest of our government's intelligence organizations is the National Security Agency (NSA). It was created by executive order on October 24, 1952. The NSA controls 85 percent of the nation's intelligence gathering assets./19/ Its budget is estimated to be as high as 10 billion dollars, and it reportedly employs as many as 68,000 people. Yet its charter and its activities remain closely guarded secrets./20/ According to the Government Accounting Office, the agency classifies somewhere between 50 and 100 million documents per year /21/, which are sealed under a blanket of secrecy created by Section 6 of Public Law 86-36 (1959)

The American public has very little access to any information held b, this agency, nor does Congress. In fact, the only judicial review of the activities of the NSA, and of the uses it makes of its information, is done by the Federal Intelligence Surveillance Court which sits in secret in a windowless room on the top floor of the Justice Department building. It does not publish public opinions and the only lawyers who argue before it are government lawyers.

The NSA monitors international communications for an absolutely vital reason: national security. However, its capabilities are awesome, and its director himself agreed that it is technologically possible for the agency to monitor domestic communications with computerized listening capabilities./22/ The agency monitors international communications which

originate within the U.S. or enter the U.S. from other countries. Through surveillance techniques made possible through enormous technological advances, the NSA has issued about 3900 reports to other federal agencies concerning 'watchlisted' Americans between 1967 and 1973./23/ These reports concerned such matters as drug dealing, terrorist activities, organized crime and organizations engaged in anti-war and civil rights activities.

In reference to the NSA's technological capabilities, Senator Frank Church stated that:

> At the same time, that capability at any time could be turned around on the American people and no American would have any privacy left, such (is) the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide. If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back, because the most careful effort to combine together in resistence to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capability of this technology. . ./24/

Philosphical and Legal Issues

Implicated in the Concept Privacy

In view of the changes in technology that we face, three possibilities about the relationship between law and technology must be explored in order to further define the problems at hand and to propose solutions.

First, technology may be illustrating to us that our underlying assumptions about the law are wrong. We simply cannot control information about ourselves. The idea that we could was a product of a simpler age.

Second, technology is forcing the law to alter or abondon itself altogether. This relationship can be illustrated by the common law's abandonment of the old legal notion of a right to property ad coelum, where the emergence of the airplane and its utility forced the common law to abandon the notion that land owners had right to their land which extended to the heavens./25/

Third, technology may be forcing us to a deeper understanding of the law.

The first and second proposition, at first impression, appear to be quite true. If the underlying axiom concerning privacy is the right to control information about oneself, or for that matter, an idea of expectation of privacy, we must concede that the revolution in information technology has made privacy an impractical, if not impossible, interest to define and assert. The situation is analogous to the advent of the airplane and the fate of rights to property ad coelum. But should the law abandon the right of privacy? To answer this, an analysis of the third proposition is necessary.

Adressing the third proposition is not an easy task. Let us take a simple example of an invasion of privacy, the peeping tom, and try to identify its components. Stripping the problem of its property rights aspects, what is left? What harm does the peeping tom cause? Who suffers and when do they suffer?

The peeping tom creates a threat in three ways to the person observed. The first level of threat has to do with survival. The other two threats have to do with perceptions.

Regardless of our intellectual capabilities, we are creatures who depend upon an environment for our existence. We exist in a physical universe and our experiences occur within the limits of space and time. On one hand, the environment is a dangerous place: in it we can befall any number of casualties. On the other hand we must be nourished by it: we are part of it. We can occupy only one place in the environment at a given time, yet, we cannot be aware of the environment all of the time. We must sleep. Instinctually, we require a refuge and isolation from the environment. Most animals in the natural kingdom seek out some place where they can rest isolated from the dangers of the environment. We are no different in that respect. The instinctual need for territory or a safe place is implicated in many kinds of privacy invasions. On this level, the need for privacy is related to a basic survival instinct.

The peeping tom creates two threats which have to do with perceptions, ego and social survival. First, the peeping tom has gained the ability to alter the perceptions of others about the person who was observed.

Second, whether or not it is true, the person observed perceives a threat stemming from the possibility that someone else can affect the perceptions of others about them. Arguably, this age old scenario represents some kind of harm in a purely psychological way. It is quite possible that psychological needs underly the idea of privacy. Very few formal studies have been done in this area. The psychologist, Sidney M. Jourard, wrote that in order for people to enjoy physical and mental health they require both a 'private place' and a 'zone of psychological privacy' in which they are free to act without sanctions in ways that disclose his or her 'being for oneself'. He writes that people need to be free from guilt stemming from the discrepancies between the way they appear in public and the way they are in private. This is so because people need freedom to experience and room to grow./26/

From a different point of view, the peeping tom scenario is one in which the law recognizes harm because of damage to the personal autonomy of the person observed, as well as to the residents in the peeping tom's community. American common law and constitutional law both have as a foundation the recognition that each person has a free will and is an autonomous entity. The philosophical and political ideology behind this foundation can be found in the writings of Locke and Mill. The ideas of free will, liberty and natural law are at the botton of our legal notions of privacy. Locke writes that the social contract is necessary because without it the enjoyment of freedom is uncertain and constantly subjected to the 'invasions of others'. Freedom to Locke was linked to a mental state of having the power of doing or forbearing to do 'according as the mind shall choose': it was 'the power of people to <u>think</u> their own actions

and to prefer their doing or omission."

We have free will, and because of this fundamental human quality, we can enjoy liberty, we have prospects, we can grow and change, and we deserve freedom from coercion. From this perspective, detailed information about the person, easily accessible in the world, creates a cast or mold which fetters the exercise of will. People need to be able to sculpt other's perceptions about them in order to exercise will and experience liberty on a fundamental level.

It is the perceived threat to autonomy that is the harm in privacy problems. This is the basic reason that the legal conceptualization of privacy is so difficult. The technology threatens our autonomy. Not only does the technology threaten our autonomy and our liberty, it has the potential to destroy it.

If the computer becomes the principal tool of communication and the medium through which we relate to each other, and if massive amounts of information about each person is stored and easily accessed, then our concepts of what it is that we are will have to change, our choices limited, and our free will impaired. We objectify ourselves when we represent ourselves to each other through data bank records. Representing ourselves through the computer negates our autonomy. We become objects--data--through which others perceive us, decide to hire or fire us, decide to associate with us and make predictive judgments about our future actions.

Society faces a serious dillema. Enormous benefits accrue from easy access to data base records. Imagine the utility of a system whereby each persons entire medical history could be put at a doctor's fingertips during emergency room treatment. Likewise, it is clear that credit records, properly maintained and accessed, are essential to good business relations. The technology is here to stay. Our national security depends on it. Yet, in order to protect our autonomy, the government must invade it. Being militarily secure in the age of information requires that the government use the means by which we are threatened. Communications technologies must be relied upon to make all decisions about protecting the soveriegn, even the deployment of nuclear weapons. The government must threaten us if it is to protect us. This explains the NSA's existence.

We are now in a position where national defense concerns are so great, considering the capabilities of nuclear warheads, that when we balance almost any harm to the individual against the need for national security, the answer is that national security prevails. What could be more important than avoiding a holocaust? Certaintly, not privacy and personal liberty.

To be able to ask the preceding question and to be forced to give the preceding answer tells us that society has a monumental problem for which we must begin to more actively explore solutions.

EXPLORING SOLUTIONS

It is a mistake to think that solutions to problems presented by information technology are to be ultimately found in regulating the collection, storage and dissemination of personal information. This approach, which is the basic approach of the FOIA, the Privacy Act of 1974, and most state statutes, is based on a paper information mentality. This is not to say that these laws are undesirable. On the contrary, they are critically important to maintaining a free society. It is to say that we must study the possible effects the technology will have on our society, and make choices about the way in which the technology should be incorporated into our lives. The tool through which this can be done is the law.

Thus, technology is forcing us to a deeper understanding of ourselves and of the law. It is forcing the scope of legal inquiry and adjudication to include a greater sensitivity to the enduring philosophical questions. The law should include processes through which the future impact of a technology on the individual can be determined. How to do this should be the topic of intensive research in legal and non-legal educational institutions. The law as it protects the individual should move quickly from a retrospective mode of operation to a prospective one.

Technology is also forcing us to a deeper understanding of political

ideology. Never before has the understanding or formulation of political ideology been more important than it is right now. Related to the information revolution in technology is the ability to link computers with machines so that they can do intelligent work. The magnitude of that concept is difficult to imagine. The basic business about which people have concerned themselves for the past two million years is the physical manipulation of the environment for the satisfaction of our material needs. Machines will soon be able to do most of the work traditionally done by people. We also will have to deal with an informational power which has the capacity to control and manipulate us. Do we have goals as a society that guide us, that point out the proper course to take?

Three possible paths lay ahead. The first possibility is that we can use technology, but probably not stop it, as a means to achieve our objectives or goals as a society. The second is that the technology, driven by its own values, and indifferent to human needs, will take its own course and drag the human race with it. The third possibility is that the technology will be controlled by a few and be used to control and to subjugate the rest.

Needless to say, the first path is the only acceptable one. On a primary level, recognizing that technology can fashion what it is that we will become is the first step down this path. The second step is to recognize that individual liberty is a major and essential objective in a democratic society and that it depends on personal autonomy. The ideal of personal autonomy must be refined and respected: it must be recognized as something greater than and different from material possessions or wealth , a healthy

economy, or the threat of nuclear holocost.

Democratic ideals are threatened in a serious way, not by the information technology itself, but by the potential that it has for de-humanizing us and destroying our heritage. Joseph Weizenbaum, a computer scientist, writes in Computer Power and Human Reason that "the computer has thus begun to be an instrument for the destruction of history. For when society legitimates only those data that are in one standard format and that can easily be told to the machine, then history, memory itself, is annihilated. . . how long will it be before what counts as fact is determined by the system, before all other knowledge, all memory, is simply declared illegitimate." /27/

The limit that we need to put on information technology is one that prevents us from becoming its subjects, its data. As a general proposition, the less we fill the computer with personal information about ourselves, the better off we will be.

On a secondary level, more comprehensive regulation of information by the states is necessary./28/ In order to prevent the psychological threat to autonomy, people need to know when information about them is kept, exchanged, used or sold. This is as important in the private sector as it is in the public. Every state regulates information in some way. At a minimum some regulate adoption and criminal records, at the maximum, others have passed open government records laws, amended their constitutions to include a right to privacy, and passed a variety of laws to protect the confidentiality of certain kinds of information.

One of the greatest threats posed by new information technologies is the growing ease with which separate record systems, each of which alone seems innocuous, can be integrated, inter-connected and even automated. To my knowlege, no laws have been passed in any state that regulate or prevent this kind of integration and compilation of personal information in the private sector. Yet power by information is menacing, regardless of who the holder is. Perhaps a technological solution can be employed in order to restrict the illegitimate flow of personal information. If communications networks can be automatically monitored, why not automatically monitor, for purposes of prevention, the unauthorized transmission of personal information. This would recognize that we are something apart from and above computerized information.

About the uses to which computers should not be put, Weizenbaum suggests: 'There are two kinds of computer applications that either ought not be undertaken at all, or, if they are contemplated, should be approached with utmost caution. These are. . .all projects that propose to substitute a computer system for a human function that involves interpersonal respect, understanding, and love. . .The second kind of computer application that ought to be avoided, or at least not undertaken without very careful forethought, is that which can easily be seen to have irreversible and not entirely forseeable side effects. . .The example I wish to cite here is that of the automatic recognition of human speech. . . ./29/

The problems we face require social and political value choices of the most basic kind. I have suggested that our interests in privacy are linked to what it is that we are and how it is that we must relate to the

physical and social environment. Information technology has the capacity to change us in a way that can impair creativity and individual autonomy; it can bring about a medium for human experience through which people can be easily manipulated. Our public decisions about information technology must take this into account, and our democratic ideals must be reaffirmed. Can our society continue to grow by building democratic institutions and allowing citizens to make voluntary choices and sacrifices, or will information technology be used as a means of social control, regardless of human choice, in ways yet to be imagined?

Solutions to the legal and philosophical questions presented herein will be difficult to reach because of the rapid changes in technology itself. The creation of new individual rights by traditional processes is too slow a process. If individual rights are to stand as a check to, or control of, information technology, they must be brought about by lawyers who can break out of categorical legal standards and who will pressure courts continuously with aggressive and innovative legal and philosophical arguments. If new rights are to come about in a meaningful way, the way in which society educates its lawyers will have to change: the shift will have to be from teaching law students how to become good technicians, to teaching them how to identify the functions and justifications of the law so that they can adapt it to the changing legal issues and categories brought about by technological advances. A lawyer should be able to readily articulate to a court the reasons why, for example, the electronic surveillance of his client in the work place is a harm for which a court should offer relief. It is not enough for the lawyer to say to the client: "you don't have a cause of action under the four categories of

invasion of privacy or under a statute--there is nothing you can do about it."

Rapid advances in technology require that the legislative process take on a greater role in the protection of individual rights and liberties. If meaningful laws are to be enacted in the area of privacy and information technology, the process through which those laws are enacted cannot be dominated by special interest groups or by national security interests. Rather, the process must be dominated by a genuine and prospective concern for the autonomy of the individual and for our liberty in society.

The way in which law should affect science and technology should be a topic of major emphasis and study in the political, academic and legal process./30/ It is one of the most important evolving areas of serious philosophical inquiry today. My point in conclusion is that addressing this question in the new age of information requires renewed attention to questions about human experience and political ideology. Only when these questions are considered as essential elements of public policy decisions, can the proper balancing of critical interests be made.

FOOTNOTES

1. Richard E. Leakey and Roger Lewin, Origins, (New York: E.P. Dutton, 1977), ch. 3.

2. For a general discussion of these definitions and their sources, see, David M. O'Brien, Privacy Law and Public Policy (New York: Praeger Publishers, 1979), pp. 3-31.

3. Samuel H. Hofstadter, The Right of Privacy (New York: Central Book Company, 1964), p. 10.

4. Hofstadter, Ibid. at p. 10.

5. 122 Ga. 190, 50 S.E. 68 (1905).

6. Samuel D. Warren and Louis D. Brandeis, The Right to Privacy, 4 Harvard Law Rev. 193 (1890).

7. Prosser, Wade & Schwartz, Cases and Materials on Torts, 6th Ed. (Mineola: The Foundation Press Inc., 1982), p.1058.

8. John M. Eger, The Global Phenomenon of Teleinformatics: An Introduction, 14 Cornell Intl. L.J. 203, 204 (1981).

9. Dorsey, Computers from the Perspective of Social Policy, Wash. U.L.Q. 379, (1977).

10. For a description of these technologies, see Time Magazine, Vol 121 No. 8, at p. 60, Feb. 21, (1983).

11. Consider the following examples of this growing industry: the Dow Jones News/Retreival; Lexix, Nexis, and Lexpat computerized legal and non-legal research services--sold by Mead Data Central, New York, New York; the Rueben H. Donnelley Corporation and the R.L. Polk Company, who both sell mailing lists compiled from public records of voter registration, telephone directories, auto registration and property ownership; the Medical Information Bureau of Boston Massachusetts, which stores personal medical records and services insurance companies; the Retail Credit Corporation of Atlanta Georgia, known as Equifax, Inc., which conducts investigations of individuals for credit, insurance, and employment purposes, and who sells the information which often includes subjective judgments about lifestyles. For a discussion of such businesses, see, generally, Robert Ellis Smith, Privacy, How to Protect What's Left of It (Garden City: Anchor Press ,1980) chapters 4,5,8,9 & 10.

12. For a Discussion of this concept in general, see, H. Hart & A. Sacks, The Legal Process: Basic Problems in the Making and Application of Law

(Tent Ed. 1958), p. 139,427,565.

13. 5 U.S.C. Sec. 552; 5 U.S.C. Sec. 552a: and 42 U.S.C. Sec. 2000aa.

14. For a collection and comparison of such laws, see, Braverman and Heppler, A Practical Review of State Open Records Laws, 49 Geo. Wash. L. Rev. 720 (1981).

15. Other technologies force us to do the same; for example, the science of genetic engineering.

16. Report of the U.S. Privacy Protection Commission, Privacy in an Information Society (1977), p. 10.

17. Smith, Ibid., at p.84.

18. Smith, Ibid., at pp. 87, 88, 89.

19. James Bamford, The Puzzle Palace, A Report on America's Most Secret Agency (Boston: Houghton Mifflin Company, 1982), p. 2.

20. Bamford, Ibid., at pp. 3 and 77.

21. Bamford, Ibid., at p. 65.

22. Bamford, Ibid., at p.301,302. Bamford reports that the NSA can monitor communications by computers which upon recognizing certain words, or groups of words, will record the communication.

23. Bamford, Ibid., at pp. 249 and 300.

24. National Broadcasting Company, "Meet The Press" (Washington D.C.: Merkle Press, 1975), transcript of August 17, 1975, p.6; Bamford, Ibid., at p. 379.

25. Hugh Gibbons, The Relationship Between Law and Science, Part I, Idea, The Journal of Law and Technology, vol. 22, no. 1, at pp. 55, and 56.

26. Sidney M. Jourard, Some Psychological Aspects of Privacy, Law and Contemporary Problems, Spring 1966.

27. Joseph Weizenbaum, Computer Power and Human Reason (San Francisco: W.H. Freeman and Co., 1976), p. 238.

28. For an excellent study and proposal of private information codes to be enacted by the states, see, Privacy, Security, and the Information Processing Industry, prepared by the Ombudsman Committee on Privacy, Los Angeles Chapter, Association for Computing Machinery. (ACM Order Dept., P.O. Box 12105, Church Street Station, NY,NY)

29. Weizenbaum, Ibid., at pp. 268 to 270.

30. This question is the major topic of inquiry by Hugh Gibbons in The Relationship Between Law and Science Part IV, Idea, The Journal of Law and

Technology, vol.22, no. 4, p.283.

• • •